CAUDIT
Council of Australasian University Directors of Information Technology

Security Legislation Amendment (Critical Infrastructure) Bill 2021

CAUDIT response
Classification: Public
01 February 2022

The Council of Australasian University Directors of Information Technology (CAUDIT), with input from its members, submits the following submission to the Department of Home Affairs on the Security Legislation Amendment (Critical Infrastructure) Bill 2021. CAUDIT continues to welcome the opportunity to provide feedback and support the outcomes from the Bill in respect to Higher Education and Research.

CAUDIT is the peak member association supporting the use of information technology and cyber technology in the higher education and research sector in Australasia. CAUDIT is a registered Not-For-Profit Association with 62 members which includes all public universities in Australia and New Zealand, those of Papua New Guinea and Fiji, and key national research organisations in Australia. Members are represented by the most senior person with strategic responsibility for Information Technology (IT) operations and digital transformation in their institution i.e., the CIOs, CDOs, and IT Directors of each member organisation.

The Australasian Higher Education Cybersecurity Service (AHECS) was formed in 2019 as a result of the CAUDIT Member Representatives (CIOs of institutions) voting cybersecurity as their number one priority for collective action. AHECS is delivered in collaboration with CAUDIT, Australia's Academic and Research Network (AARNet), AusCERT, Research and Education Advanced Network New Zealand (REANNZ), and the Australian Access Federation (AAF). AHECS is a higher education sector collective that leverages the capabilities and expertise of its partner entities to strengthen the overall cybersecurity posture of the sector. AHECS also acts as central body, representing the sector on cybersecurity issues.

AHECS's purpose is aligned to the principles of being stronger together and 'all boats lift on a rising tide'. It is a collective developed specifically for the sector by the sector to address capability gaps and help defend the sector from continuously evolving cybersecurity threats. This is achieved through coordination of members and partners to inform direction, advocate, share intelligence, reduce barriers to the implementation of good practice, identify and act on capability gaps, and holistically defend the sector from continuously evolving cyber security threats in conjunction with key vendors. AHECS aligns with, and supports, the University Foreign Interference Taskforce (UFIT) cybersecurity goals.

CAUDIT and the AHECS partners are ready and well placed to support Government cybersecurity initiatives and proactively help the higher education and research sector in Australasia in ensuring the national security risks affecting the sector are appropriately managed and addressed.

CAUDIT welcomes this opportunity to engage with the Department on the proposed critical infrastructure reforms and the Security Legislation Amendment (Critical Infrastructure) Bill 2021. CAUDIT supports the Australian Government's vision for critical infrastructure security and resilience.

After discussion with our members, CAUDIT's response to the Bill notes the following key recommendations:

1. Reporting guidelines for other cybersecurity incidents.

The amendment notes the requirement to report both *critical* and *other* cybersecurity incidents, with set timeframes for each. While the definition of critical cybersecurity incidents is reasonably clear, CAUDIT and our members note the documented definition of *other* cybersecurity is ambiguous. CAUDIT supports the clarity with critical cybersecurity incidents only being reported if they affect the availability of a critical asset.

The ACSC online reporting form notes some examples of these incidents which includes malicious emails, brute force attempts, unauthorised access attempts, and denial of service attacks. The volume of reporting associated with these examples, and all *other* cybersecurity incidents per the current definition, is likely to lead to unnecessary overreporting, putting pressure on our members and Departmental resources, without providing benefit to the Governments objective to safeguard critical infrastructure.

The Explanatory Memorandum states that 'The Department will provide further guidance and support to industry to assist with identifying what is a significant impact for the purpose of this section in different sectoral contexts.'. We have not seen any published guidance from the Department in relation to the university sector. Presumably, this will be provided as a part of the current consultation phase on the Draft Application Rule or during the period leading up to the commencement of mandatory notification obligation (being three months from the date they are 'switched on').

To ensure the process for cybersecurity incident reporting is effective, actionable, valuable, and members can remain compliant with their legislative requirements, CAUDIT notes our members would greatly appreciate clarity regarding the definition of *other* cybersecurity incidents. This may include a framework or risk-based threshold to further outline their reporting requirements per the *other* cybersecurity incident category. The use of "imminent" suggests the timing of events that may occur in the future. Changing this phrasing to "probable" would allow a risk-based approach when reporting.

Recommendation: We recommend that the Government further define '*other*' cybersecurity incidents to avoid overreporting, and to ensure the effectiveness of the process including the best use of the sector and the Departments incident response resources.

2. National/global cybersecurity incidents and cloud services reporting

Many institutions use similar service providers, and, as such, using the current reporting guidelines, the Department would be faced with an influx of cybersecurity incident reports if a service provider experienced a cybersecurity incident or technical fault which impacted the institutions services, particularly the use of cloud services and incidents compromising service availability. Likewise, similar overreporting would occur in the event of a service provider experiencing a national or global incident or service outage.

Given the service provider would have pertinent information regarding cybersecurity incidents impacting their organisation, overreporting in these situations would be of limited value, would utilise unnecessary resources (both from institutions, and the Department), and would distract key staff from the incident response. We recommend it would be more effective to limit reporting requirements in these circumstances to only cases where data is compromised or exposed at an institution. In other words, we recommend the Department refine the reporting guidelines to note institutions are not accountable to report in these cases unless the incident involves their data.

Recommendation: We recommend the mandatory cybersecurity incidents reporting requirements be further defined to exclude cybersecurity incidents at a service provider level (including cloud services), unless the incident impacts (i.e., compromises or exposes) the institutions data.

3. Definition of critical assets

During discussions with members, we note variances in the interpretation and the process of defining critical services, and assets under Part 2 of the SOCI act. Whilst some institutions have conducted business impact assessments to define their critical assets, others would appreciate clearer definitions of the assets relevant to national significance. For example, should assets that are critical to the institution automatically be deemed as critical to national significance?

Per the Government objectives, we recommend research assets and university services (i.e., availability of teaching resources or research systems) that directly affect the institutional capability to deliver the services be noted as critical, with general education assets or ancillary systems excluded (i.e., support systems that do not impact the service, incidents affecting an individual staff member or student). The Departments experience with existing Critical Infrastructure sectors could be utilised to provide clear guidance.

Recommendation: We recommend the Department clarify the definition of critical assets, to ensure consistency in reporting across the sector.

4. Ease of reporting

Cybersecurity incidents can be reported either via phone or using an online form, and these multiple reporting options are appreciated. We note it is imperative for the reporting process to be effective and not onerous, keeping in mind that the reporters are likely simultaneously managing their own incident response processes as part of the reportable cybersecurity incident. As such, we hope the Department considers these opportunities to improve the logistics of the reporting process and continues to maintain the following key reporting functionality:

- After submission (via either the phone or online form), the reporter should receive an email record of the information they have provided.
- When using the online form, the reporter should be able to ‘save’ draft, or the form should be limited to basic mandatory fields, allowing the reporter to initially submit using the key information only.
- The online form should include a checkbox to note whether the submission is of a critical, or other nature.

- The Government provide an additional open-format, technology enabled automated reporting mechanism, and support financial assistance for institutions to ensure automatic report of incidents is an option. This would align with providing timely reporting while supporting institutional focus on addressing the incident.

We also recommend an avenue/opportunity to provide feedback on the reporting process and the associated outcomes with the Department, following any reported incidents.

Recommendation: We recommend the Department continues to monitor and review the online submission process to ensure the logistics for reporters is effective and manageable.

Thank you for the opportunity to provide feedback on the Security Legislation Amendment (Critical Infrastructure) Act 2021.

If you would like further information, or to explore any of these comments, please contact:

Greg Sawyer
Interim Chief Executive Officer
Council of Australasian University Directors of Information Technology (CAUDIT)
[redacted]